CLAIMS

1. A remote computer forensic evidence collection apparatus, comprising:

a mechanism for remotely collecting client data while adhering to strict evidentiary standards; and

a mechanism for automatically verifying content received from a victim machine with data from said victim machine.

2. The apparatus of Claim 1, said system comprising:

a forensic evidence aggregator;

an image generation system; and

a bootable image containing a forensic evidence collection suite.

3. The apparatus of Claim 2, wherein said image generation system comprises:

a set of scripts that gather any of the following information from said victim machine:

network configuration; system architecture; and media device configuration.

4. The apparatus of Claim 2, wherein said image generation system comprises:

a set of scripts that take information concerning said victim machine and generate a bootable image for said victim machine from an appropriate machine kernel.

5. The apparatus of Claim 2, wherein said image generation system comprises:

a set of scripts that generate a one-use certificate for authentication and authorization that allows a single connection to said evidence aggregation server from said victim machine.

6. The apparatus of Claim 2, wherein said forensic evidence aggregator comprises:

an SSL server that restricts connections based upon verification of a certificate by a trusted third party authority.

7. The apparatus of Claim 2, wherein said forensic evidence aggregator comprises:

a server that provides multiple disk support, such that each host has it's own physical disk that is stored separately, where each such disk has it's own chain of custody.

8. A remote computer forensic evidence collection method, comprising the steps of:

a client contacting an incident response team when a security incident is suspected to have occurred, wherein said incident response team is provided with any of the following information:

system architecture for a victim machine;

network configuration of said victim machine;

access control devices on a network to which the victim machine is connected; and

why an incident is suspected;

said incident response team entering relevant data into a script to generate a kernel boot image for said victim machine;

said incident response team providing said client with a one-time password;

said client accessing an on-line signing authority with said one-time password and downloading said kernel boot image onto a storage medium, wherein said kernel boot image is encrypted using an encryption application and an encrypted version of said kernel boot image is sent to said client;

said client rebooting said victim machine using said kernel boot image on said storage medium, wherein all media associated with said victim machine are mounted in read only mode and wherein said victim machine can establish network connectivity;

taking a first cryptographic hash of all of essential partitions on said victim machine;

sending said cryptographic hashes to an evidence aggregation server and, optionally, to any of a trusted third party and a time stamping authority;

retrieving data from said victim machine and streaming said data to said evidence aggregation server via a secure connection;

storing said data at said evidence aggregation server on a partitioned, separable storage medium;

once streaming of an image of said victim machine data to said evidence aggregation server is completed, taking a cryptographic hash of said data on said evidence aggregation server and comparing said cryptographic hash with said first cryptographic hash; wherein if said cryptographic hashes match, a secured email is sent by said evidence aggregation server indicating that an image of said victim machine has been captured has captured successfully; and

removing said separable storage medium from said evidence aggregation server and remitting said separable storage medium to a chain of custody.

9. A method for securing a victim machine, comprising the steps of:

running said victim machine from a secure boot disk, such that a state of all machine resources remains unchanged from a time an incident is first reported;

said secure boot disk operating said victim machine to produce a first hash of said victim machine contents, wherein said hash is sent to a trusted authority;

said victim machine streaming said victim machine contents to a remote location where they are securely stored;

once said victim machine contents are captured at said remote location, performing a second hash of said victim machine contents as received at said remote location and comparing said second and said first hashes to determine whether or not said captured victim machine contents provide a true representation of said victim machine contents;

wherein if a match is determined, then passing said victim machine contents captured at said remote location through a chain of custody that securely retains its authenticity.

10. A forensic disk image, comprising:

a bootable kernel that is selected for a victim machine from multiple machine architectures to provide support for networking and multiple drive configurations, wherein said disk image is protected so that it mounts in a read only mode;

a message digest function to be performed by software on said disk image to volumes on said victim machine to be copied therefrom for remote forensic analysis, wherein message digest creates a unique and non-reputable identifier for data to be copied for a third party signing authority;

an optional mechanism for synchronizing a system clock of said victim machine so that time stamps are accurate;

a one time use certificate signed by a trusted authority for limiting a connection available from said victim machine to a single session with an evidence aggregation server; and

a mechanism for copying contents of said victim machine over a secure channel to said evidence aggregation server.

11. A method for operating a forensic disk image, comprising the steps of:

booting and loading said disk image only into RAM of a victim machine;

detecting media devices in a read only mode;

bringing up network support , wherein no services are turned on, so said victim machine is secure;

optionally synchronizing victim machine system time to an NNTP server;

establishing a secure connection to a secure server;

writing a message digest across said secure connection to a partitioned, separable storage medium on a secure server;

optionally taking timestamps and writing said timestamps to said separable storage medium on said secure server;

taking an image of said victim machine and sending said image over said secure connection to said separable storage medium on said secure server.

12. The method of Claim 11, wherein a medium containing said disk image is ejected from said victim machine and said victim machines is powered off, once sending of said victim machine image to said secure server is completed.

13. The method of Claim 11, wherein said separable storage medium on said secure server is removed from said secure server and a chain of custody is created, once sending of said victim machine image to said secure server is completed.